



Diese Meldung wurde von [presstext.deutschland](http://www.presstext.de) ausgedruckt und ist unter <http://www.presstext.de/pte.mc?pte=080409039> abrufbar.

IKARUS Security Software warnt vor zu sorglosem Umgang mit Web 2.0

Facebook und Co als ideale Plattformen für Cyber-Angreifer

Wien (pts/09.04.2008/15:34) - Mit Web.2.0 wurde das große "Socialising" Zeitalter eingeläutet. Nicht, dass die Leute nicht auch schon früher miteinander gesprochen hätten - nur jetzt tun sie es für alle anderen auch zum Nachlesen. Wobei die eigentliche Intention von Flickr, youTube, mySpace, Facebook und Co ja eine wirklich geniale ist: Mit Freunden und Familie in Verbindung bleiben, Fotos und Videos tauschen und freigeben, ehemalige Klassenkameraden, Freunde, Mitarbeiter wiederfinden, über Interessen und Hobbys diskutieren, Partys und andere Veranstaltungen planen; neue Freunde finden und und und. Diese Features beschere den meisten 2.0-Applikationen enorme Zuwachsraten.



Nur leider erleichtert der unbekümmerte Umgang mit diesen Einrichtungen neue Attacken in Form von Viren, Trojanern und Spam.

Rund 52 Millionen Menschen nutzen Facebook und die Anzahl der Anwender verdreifacht sich pro Jahr. Gar 200 Millionen Menschen sollen schon MySpace für ihren individuellen Auftritt im Web 2.0. nutzen. Aber nicht nur zum Privatvergnügen - auch Business-Communities wie XING, mit immerhin noch 4,8 Millionen Nutzern, boomen. Soviel "Erfolg" zieht unvermeidbar auch Zeitgenossen an, die aus der Gutgläubigkeit vieler Anwender Ihren eigenen Nutzen ziehen, wie Analysen bei IKARUS ergaben.

mySpace, XING und Co sind die idealen "Research"-, "Manipulation"- und "Attack"-Plattformen für Angreifer. Auf keiner Plattform können Informationen so leicht "abgestaubt" werden wie hier. So einfach wie im Web2.0 lassen sich nirgendwo persönliche Daten verknüpfen und komplette "Profile" von Menschen erstellen. So ermöglicht etwa die Standardfreigabe auf XING unkompliziert die Netzwerke und Aktivitäten von Anwender in und um jene nachzuvollziehen. Aber auch immer mehr Netzwerk-Visualisierungs Tools erleichtern den zielgerichteten Angriff - so ist es selbst weniger versierten Angreifern möglich sich automatische "Netzwerk-Diagramme" über potenzielle "Opfer" erstellen zu lassen.

Die vermeintliche "Vertrauensstellung" führt auch dazu, dass das Verhalten von potenziellen Opfern "gesteuert" werden kann bzw. "vorhersehbar" wird - was weiter führende Attacken ungleich erleichtert und auch die Security Policies von Unternehmen massiv zu unterlaufen vermag. Web 2.0 Plattformen sind die ideale Angriffsplattform für eine Vielzahl von Attacken auch gegen Unternehmen, in jenen die Nutzer von youTube & Co ihre Arbeit verrichten. So lassen sich in vielen Fällen Firewalls "tunneln" und ContentSecurity Lösungen am Gateway unterlaufen.

Die Fülle an Daten, die freiwillig online gestellt werden, wirkt sich auch auf die Qualität von Spam aus - die Option Email-Adressbücher und ganze PSTs online zu stellen und mit "Freunden" abzugleichen und zu verlinken, trägt nicht unwesentlich dazu bei, dass Spammer reale Email Adressen einsammeln können, sondern in Verbindung mit anderen Daten auch, dass Spam immer "zielgerichteter" zum Einsatz kommt und begünstigt "Spear-Phishing" und "targeted Spam".

Einmal völlig davon abgesehen, dass vielen - vor allem jungen Anwendern - kaum bewusst ist, welche Konsequenzen ein informationsreiches "Profil" auf einer jener Plattformen später einmal haben kann - so "schick" es heute auch erscheinen mag.

Wie schade, dass ein so genialer Gedanke so zur Falle werden kann.

<http://www.ikarus.at> (Ende)

Aussender: IKARUS Security Software GmbH
Ansprechpartner: Sonja Judith Fink
email: fink.s@ikarus.at
Tel. +43-1-58995-0